European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting

W. Gregory Voss

European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting

*By W. Gregory Voss**

I. Introduction

Some of the most significant European data privacy law developments that have emerged since the European Union adopted the Data Protection Directive[1] in 1995 occurred during the past year. These include the adoption of the European Union's General Data Protection Regulation ("GDPR"),[2] the invalidation by the *Schrems* decision of the U.S.–EU Safe Harbor cross-border data-transfer framework,[3] and the subsequent replacement of the Safe Harbor framework with the EU-U.S. Privacy Shield.[4] The "right to delisting," which the 2014 *Google Spain* decision created, also experienced continued development.[5] This survey reviews the GDPR's main provisions—arguably the most important recent development—and then discusses the other developments noted above.

II. Adoption of the General Data Protection Regulation

On April 27, 2016, the European Union finally adopted the GDPR, more than four years after the European Commission proposed it. The regulation came into

* W. Gregory Voss is a professor of business law at Toulouse University, Toulouse Business School, and an associate member of the Institut de Recherche en Droit Européen International et Comparé (IRDEIC) in Toulouse, France.

1. Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) [hereinafter Directive 95/46].

2. Commission Regulation 2016/679 of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

3. Case C-362/14, Schrems v. Data Prot. Comm'r (Oct. 6, 2015), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62014CJ0362.

4. *Transatlantic Data Flows: Restoring Trust Through Strong Safeguards*, COM (2016) 117 final (Feb. 29, 2016) [hereinafter *Transatlantic Data Flows*].

5. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. 317, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131. Here, the term "right to delisting" has been preferred as the specific reference to one of the forms of the "right to be forgotten," as proposed in Voss and Castets-Renard's taxonomy. *See* W. Gregory Voss & Céline Castets-Renard, *Proposal for an International Taxonomy on the Various Forms of the "Right to Be Forgotten": A Study on the Convergence of Norms*, 14 Colo. Tech. L.J. 281, 325–27 (2016).

force on May 24, 2016,[6] and it will become applicable starting May 25, 2018,[7] when it will repeal the current Data Protection Directive.[8] This gives companies until May 2018 to adapt to its new provisions.

European Union data protection law protects individuals (natural persons, as opposed to corporate entities or legal persons), which it refers to as "data subjects," with respect to their personal data processing.[9] The GDPR defines both "processing" and "personal data" broadly and in adherence with the Data Protection Directive, even though it reorganizes and updates the Data Protection Directive's definitions. Processing with respect to personal data may include, but is not limited to, the following: "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[10] The relevant personal data are "any information relating to an identified or identifiable natural person ('data subject')," and may include location data, online identifiers, and other forms of information that may be used to identify a data subject directly or indirectly, in addition to classic identifying data such as names and identification numbers.[11]

The following sections address a few of the GDPR provisions that differ significantly from the Data Protection Directive and are important for businesses.

A. Territorial Scope

The GDPR's territorial scope is larger than that of the Data Protection Directive. The personal data processing place no longer controls the analysis; instead, under the GDPR, processing merely must occur "in the context of the activities of an establishment of a controller or a processor in the Union," a definition that expands the analysis to include the activities of the processor that processes personal data on behalf of the data controller.[12] The GDPR also applies to the "processing of personal data of data subjects who are in the [European] Union by a controller or processor not established in the [European] Union" so long as the processing is related to "the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union" or the monitoring of such data subjects' behavior "as far as their behaviour takes

6. GDPR, *supra* note 2, art. 99(1), at 87 ("This regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*."). The date of its publication in the *Official Journal of the European Union* was May 4, 2016.

7. *Id.* art. 99(2), at 87.

8. *Id.* art. 94(1), at 86.

9. *Id.* art. 1(1)–(2), at 32; *id.* art. 4(1), at 33.

10. *Id.* art. 4(2), at 33. *Compare* Directive 95/46, *supra* note 1, art. 2(b), at 38 (defining "processing of personal data").

11. GDPR, *supra* note 2, art. 4(1), at 33. *Compare* Directive 95/46, *supra* note 1, art. 2(a), at 38 (defining "personal data").

12. GDPR, *supra* note 2, art. 3(1), at 32. *Compare* Directive 95/46, *supra* note 1, art. 3, at 39 (addressing scope). The consideration of a processor's activities in determining the territorial scope of the GDPR reflects the greater accountability of processors under the GDPR, when compared to the Data Protection Directive.

place within the [European] Union."[13] For example, the GDPR applies to a U.S. provider's cloud-based-services offering to individuals in the European Union, even where the offering requires no payment and the provider has no establishment in the European Union, to the extent that the offering involves processing those individuals' personal data.

B. Personal Data Processing Principles

Although the GDPR's personal data processing principles are similar to those in the Data Protection Directive, there are a few differences. For example, the GDPR explicitly requires data to be processed "in a transparent manner," but the Data Protection Directive only implicitly requires transparency.[14] In addition, the GDPR specifies that inaccurate data must be erased or rectified "without delay,"[15] adding a time element to the "accuracy" principle already contained in the Data Protection Directive. Finally, the "accountability" principle requires the controller to be able to demonstrate compliance with the other personal data processing principles.[16] This latter provision ties into the new GDPR record-keeping obligations discussed in Section II.G.

C. Storage of Personal Data for Public Interest, Scientific, Historical, or Statistical Purposes

The GDPR also amends the "storage limitation" principle. Whereas the Data Protection Directive allowed Member States to determine personal data storage periods for "historical, statistical or scientific use,"[17] the GDPR establishes a specific regime for personal data processing "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes."[18] It exempts such data from the general requirement that personal data may only be kept in identifiable form "for no longer than is necessary for the purposes for which the[y] . . . are processed."[19] Instead, the data may be stored for longer periods subject to "implementation of the appropriate technical and organisational measures required . . . to safeguard the rights and freedoms of the data subject."[20] These measures implement the "data minimization" principle, and they may include the use of pseudonymization (for de-identification), where relevant.[21]

In addition, the GDPR allows Member States or the European Union to derogate from a data subject's rights to access or correct his or her personal data, and

13. GDPR, *supra* note 2, art. 3(2), at 33.
14. GDPR, *supra* note 2, art. 5(1)(a), at 35 ("processed lawfully, fairly and in a transparent manner"). *Compare* Directive 95/46, *supra* note 1, art. 6(1)(a), at 40 ("processed fairly and lawfully").
15. GDPR, *supra* note 2, art. 5(1)(d), at 35. *Compare* Directive 95/46, *supra* note 1, art. 6(1)(d), at 40.
16. GDPR, *supra* note 2, art. 5(2), at 36.
17. Directive 95/46, *supra* note 1, art. 6(1)(e), at 40.
18. GDPR, *supra* note 2, art. 5(1)(e), at 36.
19. *Id.*
20. *Id.*
21. *Id.* art. 89(1), at 84–85.

object to or restrict its processing, where the derogation is for scientific or historical research purpose—or statistical purposes if the data subject's exercise of such rights is "likely to render impossible or seriously impair the achievement of the specific purposes,"[22] subject to the safeguards mentioned above. Another provision permits certain derogations for archiving purposes in the public interest.[23] Where the processing has multiple purposes, the derogation will only apply to the corresponding purposes.[24]

D. Legitimate Processing Bases, Including Consent

The GDPR retains the requirement that a legitimate basis must exist in order for personal data processing to be lawful.[25] It further develops the "purpose limitation" principle, allowing the controller to evaluate whether personal data processing for a purpose other than the one for which the data were originally collected enjoys such a basis, where it is not based on the law or the data subject's consent. This compatibility determination considers, among other things, links between the two purposes, context (including the relationship between the data subject and the controller), the data's nature (specifically, whether special data categories are involved), possible consequences for the data subject, and the existence of "appropriate safeguards," which could include data encryption or pseudonymization.[26]

Where consent is the processing basis, it must be unambiguous. The Data Protection Directive provided that "the data subject's consent" meant "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[27] The GDPR similarly defines data subject "consent" but provides the additional requirement that the data subject's wishes be "unambiguous" and manifested "by a statement or by a clear affirmative action."[28]

The GDPR sets out additional conditions for such consent beyond those contained in the Data Protection Directive, including a requirement that the controller be able to demonstrate that the data subject has given his or her consent.[29] If a declaration that covers other matters contains a consent request, the request must be clearly written and distinguishable from those matters, with one risk for non-compliance being that the declaration's consent request will be nonbinding.[30] These requirements encourage good recordkeeping and proper document drafting.

22. *Id.* art. 89(2), at 85.
23. *Id.* art. 89(3), at 85.
24. *Id.* art. 89(4), at 85.
25. *Id.* art. 6, at 36–37. *Compare* Directive 95/46, *supra* note 1, art. 7(f), at 40 ("[P]ersonal data may be processed only if . . . processing is necessary for the purposes of the *legitimate* interests pursued by the controller or by the third party . . . .") (emphasis added).
26. GDPR, *supra* note 2, art. 6(4), at 37.
27. Directive 95/46, *supra* note 1, art. 2(h), at 39.
28. GDPR, *supra* note 2, art. 4(11), at 34.
29. *Id.* art. 7(1), at 37.
30. *Id.* art. 7(2), at 37.

Under the GDPR, data subjects also must be informed of their right to withdraw consent prospectively, and this right must be as easy to exercise as it was for the data subject to initially give consent.[31] When determining whether a data subject has freely given consent, a reviewing authority will take "utmost account" of whether contract performance (including for a service) "is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."[32] Finally, where a child under sixteen years old is concerned, processing is lawful only if "the holder of parental responsibility over the child" gives or authorizes consent. Member States may lower this age threshold to no lower than thirteen.[33] The controller must make reasonable efforts to verify that any such holder has given or authorized consent.[34]

E. Data-Subject Rights

The GDPR requires transparency in the provision of information to data subjects about their rights and the means of exercising them.[35] This requirement applies regardless of whether data are collected directly from the data subject[36] or indirectly from a third party.[37] Under the GDPR, data subjects continue to benefit from rights they had under the Data Protection Directive, such as the right to access,[38] the right to object to processing (which they may exercise at any time when the processing is for direct-marketing purposes),[39] and from the transparency- and accuracy-principle requirements discussed above, as well as the related right to rectification "without undue delay."[40] A data subject has the right not to be subject to a "decision based solely on automated processing including profiling, which produces legal effects concerning him or her or . . . significantly affects him or her," subject to certain exceptions, such as where the data subject provides explicit consent or where automated processing is necessary for a contract between the controller and the data subject.[41]

The GDPR creates several new rights for data subjects beyond those provided by the Data Protection Directive. First, it creates a "[r]ight to erasure ('right to be forgotten')."[42] This right is often dependent on the data subject meeting the criteria set out in the relevant clause (e.g., it is subject to there being no overriding legitimate grounds for the processing, where the data subject exercises his or

31. *Id.* art. 7(3), at 37.
32. *Id.* art. 7(4), at 37.
33. *Id.* art. 8(1), at 37. The age sixteen threshold specified in this provision does not affect the general law relating to the legal capacity of a child to enter a contract. *Id.* art. 8(3), at 38.
34. *Id.* art. 8(2), at 38.
35. *Id.* art. 12, at 39–40.
36. *Id.* art. 13, at 40–41.
37. *Id.* art. 14, at 41–42.
38. *Id.* art. 15, at 43. *Compare* Directive 95/46, *supra* note 1, art. 12, at 42.
39. GDPR, *supra* note 2, art. 21, at 45–46. *Compare* Directive 95/46, *supra* note 1, art. 14, at 42–43.
40. GDPR, *supra* note 2, art. 16, at 43. *Compare* Directive 95/46, *supra* note 1, art. 12(b), at 42.
41. GDPR, *supra* note 2, art. 22, at 46. *Compare* Directive 95/46, *supra* note 1, art. 15, at 43.
42. GDPR, *supra* note 2, art. 17, at 43–44; *see also* Voss & Castets-Renard, *supra* note 5, at 297–98, 334–36 (terming the "right to be forgotten" as including a "right to digital oblivion").

her right to object to it[43]), and may become inapplicable where processing is necessary for exercising the right of freedom of expression and information,[44] for certain reasons based on the public interest,[45] or for establishing, exercising, or defending legal claims.[46] Furthermore, "taking account of available technology and the cost of implementation," a controller that has made data public before being required to erase it shall take "reasonable steps . . . to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of," such data.[47]

Moreover, a right to restrict processing may apply, either for a period of time for purposes set out in Article 18 of the GDPR, or as an alternative to data erasure.[48] The GDPR also creates a right to data portability, which allows data subjects to request the controller to return their data in a commonly used, machine-readable format, and to request that the controller transmit such data to another controller if the processing was based on consent and was carried out by automated means.[49] The right does not apply to processing that was necessary for public interest or official authority tasks, and it must not "adversely affect the rights and freedoms of others."[50]

Finally, European Union or Member State law may restrict certain data subject rights when the restriction "respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society" to safeguard, among other things, national security, defense, the fight against crime, and the furtherance of justice.[51]

F. Responsibilities: Controllers, Joint Controllers, and Processors

Under the GDPR, most data protection obligations remain the responsibility of data controllers.[52] Unlike the Data Protection Directive, the GDPR explicitly requires joint controllers to allocate (likely through a written contract) compliance

43. GDPR, *supra* note 2, art. 17(1)(c), at 44.
44. *Id.* art. 17(3)(a), at 44.
45. *Id.* art. 17(3)(b)–(d), at 44.
46. *Id.* art. 17(3)(e), at 44.
47. *Id.* art. 17(2), at 44.
48. *Id.* art. 18, at 44–45.
49. *Id.* art. 20(1)–(2), at 45.
50. *Id.* art. 20(3)–(4), at 45.
51. *Id.* art. 23, at 46–47. The GDPR was part of a legislative package that includes a directive regarding data protection specifically in the context of justice and the fight against crime that entered into force on May 5, 2016, and must be implemented in Member State national law by May 6, 2018: Directive (EU) 2016/280 of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 119) 89 (EU).
52. GDPR, *supra* note 2, art. 24, at 47; *see, e.g.*, *id.* art. 7(1), at 37. The various data subject rights discussed above refer consistently to action to be taken by the controller. *See, e.g.*, *id.* art. 12, at 39–40.

responsibilities between them, although data subjects may exercise their rights against each of them.[53] In addition, the GDPR sets forth certain processor responsibilities, such as imposing them when a processor engages another processor, which might occur in complex processing activities.[54] Both controllers and processors must cooperate with supervisory authorities upon request,[55] and both are responsible for processing security (including, where appropriate, encryption, pseudonymization, testing, etc.).[56] If a controller or processor is not established in the European Union, but falls within the territorial scope of the GDPR under Article 3(2), as discussed above, it will have to designate a representative to receive communications from data subjects and supervisory authorities, unless an exception applies.[57]

G. Recordkeeping; Data Protection by Design and by Default

The GDPR does away with the Data Protection Directive's requirement that controllers notify supervisory authorities before carrying out processing activities,[58] but it imposes new recordkeeping obligations.[59] Recordkeeping obligations regarding processing activities (and cross-border data transfers outside of the European Union, where applicable) apply to both controllers and processors.[60] These recordkeeping requirements should not be viewed in isolation and apply to requirements that demonstrate compliance (such as where a data subject has given consent to processing) and transparency requirements, discussed above.

In addition to compliance obligations related to recordkeeping requirements, a new provision obliges controllers to "implement appropriate technical and organisational measures" to ensure data protection by design and by default, incorporating data protection principles such as data minimization.[61] Controllers may rely on voluntary certification by an approved certification mechanism as an element to demonstrate compliance.[62]

53. *Id.* art. 26, at 48.
54. *Id.* art. 28, at 49–50.
55. *Id.* art. 31, at 51. A "supervisory authority" is an independent public authority "responsible for monitoring the application" of the GDPR so as to protect data subjects' data protection rights, which are considered "fundamental rights." *Id.* art. 51(1), at 65. An example would be the French data protection authority—the CNIL. *See* W. Gregory Voss, *After* Google Spain *and* Charlie Hebdo*: The Continuing Evolution of European Union Data Privacy Law in a Time of Change*, 71 Bus. Law. 281, 283–84 (2015).
56. GDPR, *supra* note 2, art. 32, at 51–52.
57. *Id.* art. 27, at 48–49. The relevant exception for companies concerns "occasional" processing and does not include large-scale processing of certain sensitive data. *See id.* art. 27(2)(a), at 48.
58. Directive 95/46, *supra* note 1, art. 18, at 43–44.
59. *See* W. Gregory Voss & Katherine Woodcock, Navigating EU Privacy and Data Protection Laws 51 (2015).
60. GDPR, *supra* note 2, art. 30, at 50–51.
61. *Id.* art. 25(1)–(2), at 48.
62. *Id.* art. 25(3), at 48.

H. Data Protection Impact Assessments; Prior Consultation; Data Protection Officers

The GDPR introduces a new requirement under which controllers must conduct a data protection impact assessment ("DPIA") regarding proposed processing operations' impact where "a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons."[63] A DPIA is required where profiling is concerned,[64] where there is large-scale processing of special, sensitive-data categories,[65] and for data relating to criminal convictions or offenses.[66] A DPIA requires four elements:

- a systematic description of the processing;
- evaluation or assessment of the respective risks referred to above;
- measures to address the risk (including safeguards, security measures, and mechanisms to ensure data protection and regulatory compliance); and
- an assessment of the "necessity and proportionality of the processing operations in relation to the purposes."[67]

Controllers must consult with supervisory authorities prior to engaging in processing activities in cases where a DPIA "indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk."[68] In addition, Member States may adopt laws that require consultation with—and prior authorization from—the relevant supervisory authority "in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health."[69]

If a controller or processor has core activities relating to either (a) "processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale,"[70] or (b) "processing on a large scale of special categories of data . . . and personal data relating to criminal convictions and offences,"[71] then they are required to designate a data protection officer ("DPO"), who may be an employee of the controller or processor or an external service provider hired under contract.[72] European Union or Member State law may also require DPO designation in other

63. *Id.* art. 35(1), at 53.
64. *Id.* art. 35(3)(a), at 53.
65. *Id.* art. 35(3)(b), at 53.
66. *Id.*
67. *Id.* art. 35(7), at 54.
68. *Id.* art. 36(1), at 54.
69. *Id.* art. 36(5), at 55.
70. *Id.* art. 37(1)(b), at 55.
71. *Id.* art. 37(1)(c), at 55.
72. *Id.* art. 37(6), at 55.

cases.[73] However, one DPO may serve multiple entities: "[a] group of undertakings may appoint a single [DPO] provided that a [DPO] is easily accessible from each establishment."[74] The DPO must be designated based on professional qualities and expert knowledge of data protection law and practices.[75]

The controller and the processor must also ensure that the DPO "is involved, properly and in a timely manner, in all issues which relate to the protection of personal data."[76] The DPO performs his or her duties independently, shall not be penalized or dismissed for performing his or her tasks, and reports to the highest management level.[77] DPOs are bound by an obligation of secrecy or confidentiality concerning their tasks.[78] These tasks include, *inter alia*, informing and advising the controller or processor about its obligations under the GDPR, monitoring compliance with and engaging in awareness raising and relevant staff training, and serving as the supervisory authority's contact point.[79]

I. Data Breach Notifications

Under the GDPR, the controller is obligated to notify the supervisory authority[80] of any personal data breach "without undue delay and, where feasible, not later than 72 hours after having become aware of it, . . . unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."[81] If the controller does not notify the supervisory authority within this prescribed time period, it must provide a justification for the delay.[82] The processor must notify the controller "without undue delay" after discovering a data breach,[83] and the latter must document any personal data breaches to allow the supervisory authority to verify compliance.[84] If a data breach is "likely to result in a high risk to the rights and freedoms of natural persons," the controller must also notify the relevant data subject of the breach "without undue delay,"[85] unless an exception applies.[86]

J. Enforcement via Administrative Fines

The GDPR dictates that those who are at fault for data protection violations can be charged substantial fines—in certain circumstances up to €20 million or 4 percent of an undertaking's total worldwide annual turnover in the preceding financial year,

73. *Id.* art. 37(4), at 55.
74. *Id.* art. 37(2), at 55.
75. *Id.* art. 37(5), at 55.
76. *Id.* art. 38(1), at 55.
77. *Id.* art. 38(3), at 56.
78. *Id.* art. 38(5), at 56.
79. *Id.* art. 39(1), at 56.
80. *See supra* note 55 (defining "supervisory authority").
81. GDPR, *supra* note 2, art. 33(1), at 52.
82. *Id.*
83. *Id.* art. 33(2), at 52.
84. *Id.* art. 33(5), at 52.
85. *Id.* art. 34(1), at 52.
86. *Id.* art. 34(3), at 53.

whichever is higher.[87] Companies may take measures that may result in decreased fines. For example, supervisory authorities deciding whether to impose fines—and determining fine amounts—must give due regard to, *inter alia*, (1) "any action taken by the controller or processor to mitigate the damage suffered by data subjects";[88] (2) the controller or the processor's degree of responsibility, "taking into account technical and organisational measures implemented by them";[89] and (3) adherence to approved conduct codes or certification mechanisms.[90]

The preceding sections address only a few of the GDPR's 99 articles, which also include 173 recitals. Interested parties should review the entire GDPR and use the time from now until its application to assess and prepare for the requirements placed upon them.

III. Invalidation of the Safe Harbor: The *Schrems* Case

The Data Protection Directive introduced a provision that "the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if . . . the third country in question ensures an adequate level of protection."[91] In 1995, the European Union did not consider the United States to be a country that ensured an adequate protection level for personal data.

In 2000, the U.S. Department of Commerce ("DoC") and the European Commission negotiated the U.S.–EU Safe Harbor, which the European Commission then established under an "adequacy" decision[92] in order to allow personal data transfers to U.S. companies that self-certified their compliance with the substance of EU data protection law. Companies did so by subscribing to the Safe Harbor Privacy Principles (contained in Annex I to the adequacy decision), guaranteeing certain subject rights. In *Schrems v. Data Protection Commissioner*,[93] the Court of Justice of the European Union ("ECJ") addressed concerns about access to personal data by U.S. authorities in connection with mass surveillance and subsequently invalidated the Safe Harbor, leaving thousands of companies without a legal basis for their cross-border personal data transfers.[94]

87. *Id.* art. 83(5)–(6), at 83.
88. *Id.* art. 83(2)(c), at 82.
89. *Id.* art. 83(2)(d), at 82.
90. *Id.* art. 83(2)(j), at 82.
91. Directive 95/46, *supra* note 1, art. 25(1), at 45.
92. Commission Decision 2000/520 of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000 O.J. (L 215) 7, http://eur-lex.europa.eu/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:EN:PDF.
93. Case C-362/14, Schrems v. Data Prot. Comm'r (Oct. 6, 2015), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62014CJ0362 [hereinafter Schrems]. For more information on this decision, see W. Gregory Voss, *The Future of Transatlantic Data Flows: Privacy Shield or Bust?*, 19 J. Internet L. 1, 10–11 (2016).
94. *See, e.g.*, Mark Scott, *Data Transfer Pact Between U.S. and Europe Is Ruled Invalid*, N.Y. Times (Oct. 6, 2015), http://nyti.ms/1jLWfwc.

The ECJ emphasized that "the national supervisory authorities must be able to examine, with complete independence, any claim concerning the protection of a person's rights and freedoms in regard to the processing of personal data relating to him," but found that the European Commission's Safe Harbor decision denied these powers to the DPAs.[95] The resulting Safe Harbor invalidation created uncertainty about data transfers to the United States by companies processing personal data.

EU Justice Commissioner Vra Jourová was quick to express willingness to work with the DoC "to complete a revamped data agreement,"[96] and the parties commenced negotiations on what was then referred to as "Safe Harbor 2.0."[97]

IV. The Privacy Shield

The European Commission/DoC negotiations led to the establishment of the "EU–U.S. Privacy Shield"[98] and the corresponding European Commission draft adequacy decision.[99] Attached to the draft adequacy decision are seven annexes from U.S. government entities that set out various commitments and requirements, such as increased data subject protections and greater requirements for data controllers to respect data protection principles, including purpose limitations.[100] One improvement from a data subject perspective is greater opportunity for recourse through an independent recourse mechanism provided by the data controller.[101] In addition, under this new framework, an individual data subject may invoke binding arbitration of claims pursuant to the Privacy Shield principles under certain conditions.[102] Furthermore, the Federal Trade Commission ("FTC") will review non-compliance allegations "to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated," potentially resulting in enforcement action under the FTC Act.[103] Moreover, the DoC has committed to providing greater oversight and Privacy Shield compliance monitoring.[104]

Following data protection authority comments, the parties modified the EU-U.S. Privacy Shield to include "additional clarifications on bulk collection of data,

95. *Schrems*, *supra* note 93, at paras. 99–102.

96. Mark Scott, *In Europe-U.S. Clash on Privacy, a Longstanding Schism*, N.Y. Times (Oct. 7, 2015), http://nyti.ms/1Q93iJM.

97. Voss, *supra* note 93, at 11.

98. *See Transatlantic Data Flows*, *supra* note 4, at 3.

99. Commission Implementing Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, C (2016) 4176 final (July 12, 2016) [hereinafter Draft Commission Implementing Decision], http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf.

100. *See European Commission Unveils EU-U.S. Privacy Shield*, Eur. Comm'n (Feb. 29, 2016), http://ec.europa.eu/justice/newsroom/data-protection/news/160229_en.htm.

101. *See* Draft Commission Implementing Decision, *supra* note 99, annex 2, at 21–24, http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf.

102. *Id.* at 7.

103. *Id.* at 24.

104. *See* Draft Commission Implementing Decision, *supra* note 99, annex 1, at 1–2, http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-1_en.pdf.

strengthening the Ombudsperson mechanism, and more explicit obligations on companies as regards limits on retention and onward transfers,"[105] and they adopted the final implementing decision with revised annexes.[106] The Privacy Shield became operational on August 1, 2016.[107]

V. Google and the "Right to Delisting"

In the 2014 *Google Spain* case,[108] the court granted a natural person the right to compel delisting of newspaper pages containing information prejudicial to him when Internet users searched for his name using a search engine. Google sought to limit the right's geographic scope to European web domains, while the French data protection authority ("CNIL") sought to have the delisting extended to all relevant domains including ".com." The CNIL issued an order to that effect, which Google contested, prompting the CNIL to commence a formal procedure against it.[109]

On March 10, 2016, the CNIL Restricted Committee imposed a €100,000 fine on Google. In doing so, it rejected Google's offer that it would "filter results based on the geographic origin of the person performing the search," meaning that "people using the search engine from the same country [as] the plaintiff's country [could] not access the delisted result anymore."[110] The CNIL commented that "[o]nly delisting on all of the search engine's extensions, regardless of the extension used or the geographic origin of the person performing the search, can effectively uphold" the right to privacy.[111] Google announced that it was appealing the decision to the highest French administrative court.[112]

105. See Press Release, Eur. Comm'n, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows (July 12, 2016), http://europa.eu/rapid/press-release_IP-16-2461_en.htm.

106. *See* Commission Implementing Decision of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, C (2016) 4176 final (July 12, 2016) and Annexes 1 to 7, http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf and http://ec.europa.eu/justice/data-protection/files/annexes_eu-us_privacy_shield_en.pdf.

107. *See* Press Release, Eur. Comm'n, EU-U.S. Privacy Shield Fully Operational from Today (Aug. 1, 2016), http://ec.europa.eu/justice/newsroom/data-protection/news/160801_en.htm.

108. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. 317, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&rid=14.

109. *See* Voss, *supra* note 55, at 283–84.

110. *Right to Be Delisted: The CNIL Restricted Committe Imposes a €100,000 Fine on Google*, CNIL (Mar. 24, 2016), https://www.cnil.fr/en/right-be-delisted-cnil-restricted-committee-imposes-eu100000-fine-google [hereinafter *Right to Be Delisted*]. For an unofficial translation of the decision itself, see Commission Nationale de l'Informatique et des Libertés [CNIL] Decision no. 2016-054 of Mar. 10, 2016, of the Restricted Committee Issuing Google Inc. with a Financial Penalty, https://www.cnil.fr/sites/default/files/atoms/files/d2016-054_penalty_google.pdf.

111. *Right to Be Delisted*, *supra* note 110.

112. *See* Mark Scott, *Google Appeals French Privacy Ruling*, N.Y. Times (May 19, 2016), http://nyti.ms/2527XoV ("In France, Google's appeal, which will be heard by the Conseil d'État, the country's highest administrative court, in the coming months, is unlikely to resolve the continuing standoff over people's right to privacy online. A decision in the case is expected next year.").

VI. Conclusion

The European Union has finally adopted data protection law reform, and now is the time for companies to adapt to the new landscape before the GDPR applies in May 2018. Many of the GDPR's provisions address companies' compliance obligations and require greater accountability and recordkeeping. Some provisions may require changes to internal organization (e.g., DPOs, DPIAs, and procedures that allow for proper data breach notifications). The United Kingdom's DPA issued a checklist of steps to prepare for the GDPR. These include raising awareness, documenting held personal data, reviewing privacy notices to bring them into conformity with the GDPR, checking that procedures cover all data subject rights and adapting them to cover handling data subject requests, identifying legal bases for processing, implementing systems to verify ages of children and to gather parental or guardian consent, implementing procedures regarding data breaches, designating DPOs if required, and identifying any applicable supervisory authorities.[113]

With respect to cross-border personal data transfers, companies may now self-certify under the Privacy Shield. They should monitor developments regarding the right to delisting, as this affects access to information on the Internet.

In conclusion, it is clear that EU data protection and privacy law reform over the past year will necessarily require adaptation by companies and others for years to come.

113. U.K. Info. Commissioner's Office, Preparing for the General Data Protection Regulation (GDPR): 12 Steps to Take Now 2 (Mar. 14, 2016), https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf.